IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION PAPERS

OF

PAUL NICHOLAS GARTSIDE

AND

NEIL ANDREW COWIE

FOR

GENERATING MALWARE DEFINITION DATA FOR MOBILE COMPUTING DEVICES

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to the field of data processing systems. More particularly, this invention relates to the generation of malware definition data for mobile computing devices, for example data defining computer viruses, worms, Trojans, banned files, banned words, banned images etc. for devices such as personal digital assistants, smartphones, personal data storage devices etc.

Description of the Prior Art

It is known that malware, such as computer viruses, worms, Trojans, banned files, banned words, banned images etc, provides a significant threat to data processing systems. In order to address this threat, malware scanners are provided that perform on-access or on-demand examination of computer files to determine if they are infected with malware. In order to be fully effective, it is important that the malware definition data in use should be kept as up-to-date as possible. The greatest malware threat is often posed by the most newly released malware items and up-to-date malware definition data is needed in order to detect such newly released malware items. Within the context of fixed location computing devices, such as user PCs within business networks, it is established practice and there are provided known tools (such as e-Policy Organiser produced by Network Associates, Inc) that may be used to ensure that each computer has access to the most up-to-date malware definition data quickly.

There is an increasing and accelerating use of mobile computing devices using a variety of different computing platforms. Examples of such devices are personal digital assistants (PDAs providing diary, e-mail, note taking and other functions), smartphones, personal data storage devices, and the like. The range of uses and forms of such devices is rapidly increasing and the above list is far from exhaustive.

With the increased use of mobile computing devices, it is starting to occur that malware is being released that targets such devices. A further problem is that a mobile computing device may serve to store a malware infected file that does not impact that device itself, but does cause a problem when transferred to another device.

A mobile computer device can thus act as an "typhoid Mary" in spreading malware infection.

One approach to malware scanning mobile computing devices is to download the computer files they store to a PC, and then use the malware scanner on the PC to scan those files. Whilst this works, it is slow. This slowness is made worse by the rapidly increasing data storage capacities of mobile computing devices which results in the need to transfer larger volumes of data to and from those devices for scanning.

As mentioned previously, it is also important that malware definition data should be up-to-date in order to protect against newly released malware items. Malware scanner providers expend considerable effort in rapidly providing updates to their malware definition data when a new threat occurs. A newly released computer virus, such as a mass mailing macro virus, can spread rapidly and it is important to the customers of such malware scanner providers that malware definition data which will identify such items of malware is available in a matter of hours from the release of the new malware item. Providing different sets of malware definition data targeted at different mobile computing platforms represents an additional and disadvantageous maintenance overhead and slows down the availability of updated malware definition data.

Measures which can provide malware protection for mobile computing devices and easy updating of malware definition data are strongly advantageous.

SUMMARY OF THE INVENTION

Viewed from one aspect the present invention provides a computer program product for controlling a computer to generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said computer program product comprising:

obtaining code operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected.

The invention recognises that items of malware included within malware definition data relate to relatively distinct malware classes. As examples, some malware classes are scripts, macros, EXE files, boot viruses etc. It is known within existing malware definition data to include information that classifies the malware items in this way. This classification of malware items can be used to automate the generation of device specific malware definition data for mobile computing devices. More particularly, certain mobile computing devices will be subject to certain classes of malware threat but not others, and accordingly the malware class information can be used to select the malware items from within the master set of malware definition data that should be included within a mobile computing device of specific set of malware definition data. This enables the automation of the generation of the device specific malware definition data.

Preferred embodiments of the invention utilise a fixed location computing device to perform the steps of obtaining, identifying and generating. A fixed location computing device typically has available to it permanent or quasi permanent network connections, which may be used to access an updated master malware definition data set, and sufficient processing and storage capacity to generate and store one or more mobile computing device specific malware definition data sets. The fixed location computing device can be considered to become a "parent" or "guardian" of the mobile computing devices which connect to it and to which it can transfer their updated malware definition data.

The fixed location computing device may be one that is physically remote from the mobile computing device, but can communicate with it, e.g. a security policy organising server on a network, or preferably is a fixed location computing device that has a physical connection to the mobile computing device, e.g. a user's client

computer possibly with an interface cradle for mobile computing device or the like (such as wireless connections, e.g. 802.11/Bluetooth etc.).

The regular updating of malware definition data for mobile computing devices is made more likely to be performed if it is integrated with other actions normally performed by the device user rather than requiring a specific action of its own. For this reason, preferred embodiments of the invention act to check and, if necessary, update mobile computing device malware definition data during file synchronisation operations between the fixed location computing device and the mobile computing device.

The task of the fixed location computing device to generate the device specific malware definition data for mobile computing devices is made easier by the use of profile data identifying one or more different types of mobile computing device and threat data identifying one or more classes of malware threat to which different types of mobile computing device are vulnerable. In this way, the appropriate malware definition data can be readily selected from the master malware definition data.

The task of generating the mobile computing device malware definition data is further simplified by the realisation that this data is largely dependent upon the operating system of the mobile computing device, as malware tends to be operating system specific rather than hardware device specific.

Preferred embodiments operate to detect which mobile computing devices may be connected to them, in order to prepare the appropriate device specific malware definition data, by detecting the installation of application programs intended to communicate with such mobile computing devices. As an example, the installation on a PC of a computer program known to have the function of communicating with WinCE devices may be detected and thereafter the PC malware scanning agent may act to generate WinCE malware definition data from the master set of PC malware definition data it uses itself.

The mechanisms used to detect which mobile device specific malware definition data should be generated and transferred to the mobile computing devices

may advantageously be utilised to also transfer and update malware scanning programs to the mobile computing devices for execution as native of applications by the mobile computing devices themselves. Thus, the scanner engines can be kept up-to-date by using the fixed location computer to keep the latest scanner programs available for immediate transfer to the mobile computing device as and when it is connected to that fixed location computing device.

As previously mentioned, the malware against which the mobile computing device and the fixed computing device may be protected can take a wide variety of different forms. These depend largely upon the threats posed to the particular devices concerned and include computer viruses, worms, Trojans, banned files, banned words, banned images and the like.

Viewed from further aspects the present invention also provides a method for generating mobile computing device malware definition data and an apparatus for generating mobile computing device malware definition data.

The above, and other objects, features and advantages of this invention will be apparent from the following detailed description of illustrative embodiments which is to be read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 schematically illustrates the relationship between a mobile computing device and a plurality of fixed location computer devices with which it may be directly or indirectly connected;

Figure 2 is a flow diagram illustrating a PC detecting installation of an application program for communication with a mobile computing device;

Figure 3 is a flow diagram illustrating the updating of malware definition data upon a fixed location computer and the downloading of updated scanner programs;

Figure 4 is a diagram schematically illustrating the use of master malware definition data, mobile computing device profiles and policy data to generate mobile computing device malware definition data of various forms;

Figure 5 is a flow diagram illustrating updating of malware definition data for a mobile computing device upon connection of that mobile computing device to a fixed location computer; and

Figure 6 is a diagram schematically illustrating the architecture of a general purpose computer that may be used to implement the above described techniques.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 illustrates a personal digital assistant (PDA) 2 that may be linked via a cradle 4 with a personal computer 6. The PDA 2 is one example of a mobile computing device with which the present invention may be used. Other examples would be a smartphone or a personal data storage device. It will be readily understood that many other different types of mobile computing device may also require malware protection and may utilise the present technique. The cradle 4 provides a physical connection with the PC 6. It will be appreciated that other types of connection, such as a wireless (e.g. Bluetooth) connection or an IR optical connection may also be used.

The PC 2 is a fixed location computing device that operates within a well defined and controlled computer network. The PC 6 has a network link with a security policy organising server 8, such as a server running e-Policy Organiser provided by Network Associates, Inc. The PC 6 has a loaded and active malware scanner that uses a PC scanning engine 10 and PC malware definition data 12. The widespread use of PCs is such that malware scanner providers typically concentrate a high level of resources on keeping PC malware definition data 12 up-to-date and comprehensive. Accordingly, this PC malware definition data 12 may be regarded as the master malware definition data from which malware definition data for various mobile computing devices may be derived.

The PC 6 has installed upon it application software that interfaces with the cradle 4 and the PDA 2. The installation of this application software is detected by the security

policy organising server 8 and used to configure the appropriate agent on the PC 6 to maintain at the PC 6 a PDA specific malware definition data set 14 as well as an up-to-date copy of the PDA scanner engine 16. In this example, the PDA malware definition data 14 is derived from the PC malware definition data 12 within the PC itself. Alternatively, this derivation could take place within the security policy organising server 8 with the PC 6 merely serving to download the appropriate PDA malware definition data. The PDA scanner engine 16 is updated by the scanner provider and the most up-to-date copy stored within the security policy organising server 8.

As illustrated, the security policy organising server 8 communicates with a scanner provider's FTP server 18 which it regularly polls for updated master malware definition data (PC malware definition data) and any updated scanner engine programs. When these become available, they are downloaded from the FTP server 18 to the security policy organising server 8 to be made available to the various PC agents executing on the PCs connected to that security policy organising server 8.

Figure 2 is a flow diagram illustrating installation of an application program on the PC 6. At step 20, a check is made as to whether or not an application is being installed. When an application is being installed, then processing proceeds to step 22 at which a determination is made as to whether or not the application being installed is a known application which serves to provide a link to a mobile computing device. There are a relatively small number of application programs that are provided for communication between PCs and mobile computing devices and accordingly the maintenance of a list of such applications and the detection of the installation of such applications is relatively straight forward. If the application being installed is not one that links to a mobile computing device, then the processing terminates. If the application being installed is one which links to a mobile computing device, then step 24 seeks to identify the particular mobile computing device linking application concerned. These linking application programs tend to be generic to an operating system for mobile computing devices. As an example, the installation of the PsiWin program indicates that the device that will be connected will be run using the EPOC mobile computing device operating system. Similar programs that execute upon the PC may target WinCE and Palm operating system devices. It is also possible that a particular application program

may be highly device specific in some circumstances or support multiple mobile computing device operating systems.

After the mobile device linking application has been identified at step 24, step 26 serves to generate profile data associated with the type of mobile computing device that may be expected to be connected to the PC concerned in due course. This profile data includes data identifying the different classes of malware threat to which the mobile computing device or devices concerned are vulnerable and against which the malware definition data to be produced for those mobile computing devices should protect.

At step 28, the PC serves to download the latest version of the scanner engines appropriate for the mobile computing devices which are anticipated as being in future connected to that PC and also to build one or more mobile device definition data sets (DATs). Thus, in this example, the installation of software for communicating with a mobile computing device on a PC triggers that PC to build an appropriate collection of mobile computing device malware definition data and make available scanner engine programs on the PC such that these may be provided to the mobile computing device when it is connected to the PC. It may be that the PC will force installation of the malware scanner program on the mobile computing device if one is not already installed, or alternatively merely update such a malware scanner if it is already present as soon as it connects to that PC.

Figure 3 schematically illustrates the processing performed by the PC 6 in keeping its malware protection up to date. At step 30, the PC 6 periodically polls the security policy organising server 8. When such a poll is made, step 32 determines whether or not an updated PC malware definition data set is available. If such updated malware definition data for the PC is not available, then processing proceeds to step 34 at which a check is made for any available updated scanner engines for the PC or any mobile device that may be connected to that PC. Step 36 downloads any such new scanner engine programs and applies the PC versions if included. The mobile device versions will be held by the PC for transfer to the mobile device when it connects and installation on the mobile device at that time.

If step 32 indicated that a PC malware definition data said update was available, then step 34 downloads this update to the PC and step 36 applies it to the PC. Step 38 then determines whether or not there are any mobile computing devices for which the PC is responsible for maintaining mobile computing device malware definition data. If there are no such mobile computing devices for which the PC is responsible (e.g. there are no application programs installed on the PC for communicating with such devices), then processing proceeds to step 34.

If the test at step 38 indicates that the PC is responsible for generating and maintaining up to date mobile computing device malware definition data, then processing proceeds to step 40 at which the appropriate profile data and policy data is read for the mobile computing devices concerned. The profile data will include classes of malware threat to which particular mobile computing devices are vulnerable. The policy data may include user defined settings as to how the profile data should be interpreted. In a high security environment, or with mobile computer devices known to provide a significant risk, then the policy settings may be such as to increase the number of classes of malware threat against which the mobile computing device malware definition data will be generated to protect. As an example, it may be that a particular type of mobile computing device is known to be used to transfer computer files that are intended to be executed on a PC and accordingly it is appropriate to scan for all the malware threats to which a PC may be subject even though many of these will not apply to the mobile computing device itself.

Once the profile data and associated policies have been read by step 40, they are used by step 42 to control the building of updated mobile computing device malware definition data files targeted at the selected mobile computing device threats. Thus, the PC malware definition data serves as master malware definition data including information identifying the different classes of malware threat to which particular malware items belong allowing step 42 to select the data defining the items of malware within the classes of malware threat known to pose a problem to the particular mobile computing devices concerned, or against which it is desired to protect more generally in a line with user defined policies.

Figure 4 schematically illustrates the generation of mobile computing device malware definition data from master malware definition data. In this case, the master malware definition data is the PC malware definition data 44. The PC 6 also stores profile data 46 which identifies for each operating system platform for mobile computing devices which may be connected to that PC against which classes of malware item within the master malware definition data the particular operating system should be protected. Policy data 48 includes user defined policy settings that modify the profile data. In the example illustrated for EPOC operating system devices, the malware definition data will be built to protect against the default set of classes of threat as indicated in the profile data 46. Conversely, a higher security setting is defined within the policy data 48 for WinCE devices where it is indicated that all file types should be scanned and accordingly malware definition data built for WinCE devices will include data defining malware items that will not in themselves adversely affect a WinCE device, but which could harm a device to which an infected file is passed by such a WinCE device.

There are a small subset of malware items that only adversely impact mobile computing devices and do not operate upon PCs. An example would be a computer virus specific to the Palm operating system. The master malware definition data 44 includes data defining such mobile device specific malware threats even though they would not impact a PC itself. These may be usefully provided within the data which controls how a PC scans as they are relatively few in number and the presence of such a malware item on the PC might threaten the data on an associated mobile computing device should that file be transferred to the mobile computing device concerned. The mobile computing device malware definition data sets 50, 52 that are built by the PC will include the mobile device specific malware items for the operating system platform of the device concerned. The mobile device specific malware items for other mobile computing device operating systems would not normally be included.

Figure 5 schematically illustrates the updating of a malware definition data set on a mobile computing device. At step 54, the PC 6 waits for a mobile computing device to be connected. Once such a device is detected, step 56 performs the automatic synchronisation tasks typically set up on a PC for such devices. It may be that such synchronisation does not automatically occur, or only occurs when user triggered, but

once triggered follows a predetermined form. An alternative to the synchronisation performed at step 56, or in addition to its synchronisation, would be automatic backup of a mobile computing device that is performed when it is connected to its parent PC.

At step 58, data identifying the versions of the malware definition data and malware scanner program currently installed on the mobile computing device are retrieved from the mobile computing device to the PC. At step 60, these retrieved version identifiers are compared with the identifiers for the latest versions of the mobile computing device malware definition data and mobile computing device scanner program held on the PC and kept updated in accordance with Figure 3. If an update is required, then this is detected at step 62 and step 64 then transfers the appropriate updated mobile computing device malware definition data or mobile computer device scanner program to the mobile computing device and installs it thereupon.

It will be appreciated that the PC effectively performs the role of a parent or guardian for those mobile computing devices that may be connected to it. The PC takes responsibility for making available updated malware definition data and malware scanner programs for the mobile computing device that can connected to it. The appropriate mobile computer device malware definition data may be locally built by the PC from its own malware definition data. In this way, the mobile computing device may benefit from the permanent or quasi-permanent high bandwidth communication links that are available to the PC and the methodical and secure malware protection policies, systems and practices that are provided for the PC operating within its controlled environment. Thus, the PC will typically have reliable malware definition data updates and scanner program updates which are monitored and enforced either manually by a System Administrator or automatically by a security policy organising server 8.

Figure 6 schematically illustrates a general purpose computer 200 of the type that may be used to implement the above described techniques. The general purpose computer 200 includes a central processing unit 202, a random access memory 204, a read only memory 206, a network interface card 208, a hard disk drive 210, a display driver 212 and monitor 214 and a user input/output circuit 216 with a keyboard 218 and mouse 220 all connected via a common bus 222. In operation the central processing unit 202 will execute computer program instructions that may be stored in one or more of the

random access memory 204, the read only memory 206 and the hard disk drive 210 or dynamically downloaded via the network interface card 208. The results of the processing performed may be displayed to a user via the display driver 212 and the monitor 214. User inputs for controlling the operation of the general purpose computer 200 may be received via the user input output circuit 216 from the keyboard 218 or the mouse 220. It will be appreciated that the computer program could be written in a variety of different computer languages. The computer program may be stored and distributed on a recording medium or dynamically downloaded to the general purpose computer 200. When operating under control of an appropriate computer program, the general purpose computer 200 can perform the above described techniques and can be considered to form an apparatus for performing the above described technique. The architecture of the general purpose computer 200 could vary considerably and Figure 6 is only one example.

Although illustrative embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes and modifications can be effected therein by one skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.